

## CLAIMS

What is claimed is:

- 1 1. A method for secure operation of a network device, comprising:
  - 2 (a) assigning a digital certificate to a network user;
  - 3 (b) receiving a command for operation of a network device and the digital  
4 certificate from the network user;
  - 5 (c) utilizing a cryptographic key stored in the network device to authenticate the  
6 digital certificate of the network user; and
  - 7 (d) enabling operation of the network device if the digital certificate of the  
8 network user is authenticated.
- 1 2. The method as recited in claim 1, wherein operation of the network device is  
2 enabled according to a usage policy associated with the network user.
- 1 3. The method as recited in claim 1, wherein the network device is at least one  
2 of a printer, a copier, a scanner, and a facsimile machine.
- 1 4. The method as recited in claim 1, wherein the network user approves a  
2 maintenance interaction between the network device and a maintenance  
3 administrator.
- 1 5. The method as recited in claim 1, wherein the network user is another  
2 network device.
- 1 6. The method as recited in claim 1, wherein the command for operation of the  
2 network device is encrypted, and wherein the cryptographic key is utilized to  
3 decrypt the command for operation.

09596948 061900

- 1 7. The method as recited in claim 1, further comprising receiving electronic  
2 payment for paying for operation of the network device.
- 1 8. A computer program embodied on a computer readable medium for secure  
2 operation of a network device, comprising:
- 3 (a) a code segment that assigns a digital certificate to a network user;
- 4 (b) a code segment that receives a command for operation of a network device  
5 and the digital certificate from the network user;
- 6 (c) a code segment that utilizes a cryptographic key stored in the network device  
7 to authenticate the digital certificate of the network user; and
- 8 (d) a code segment that enables operation of the network device if the digital  
9 certificate of the network user is authenticated.
- 1 9. The computer program as recited in claim 8, wherein operation of the  
2 network device is enabled according to a usage policy associated with the  
3 network user.
- 1 10. The computer program as recited in claim 8, wherein the network device is at  
2 least one of a printer, a copier, a scanner, and a facsimile machine.
- 1 11. The computer program as recited in claim 8, wherein the network user  
2 approves a maintenance interaction between the network device and a  
3 maintenance administrator.
- 1 12. The computer program as recited in claim 8, wherein the network user is  
2 another network device.

006790-2159550

1 13. The computer program as recited in claim 8, wherein the command for  
2 operation of the network device is encrypted, and wherein the cryptographic  
3 key is utilized to decrypt the command for operation.

1 14. The computer program as recited in claim 8, further comprising a code  
2 segment that receives electronic payment for paying for operation of the  
3 network device.

1 ~~15.~~ A system for secure operation of a network device, comprising:

2 (a) logic that assigns a digital certificate to a network user; and

3 (b) a network device capable of receiving a command for operation thereof and  
4 the digital certificate from the network user, wherein the network device  
5 utilizes a cryptographic key to authenticate the digital certificate of the  
6 network user;

7 (c) wherein operation of the network device is enabled if the digital certificate of  
8 the network user is authenticated.

1 16. The system as recited in claim 15, wherein operation of the network device is  
2 enabled according to a usage policy associated with the network user.

1 17. The system as recited in claim 15, wherein the network device is at least one  
2 of a printer, a copier, a scanner, and a facsimile machine.

1 18. The system as recited in claim 15, wherein the network user approves a  
2 maintenance interaction between the network device and a maintenance  
3 administrator.

1 19. The system as recited in claim 15, wherein the network user is another  
2 network device.

006590" 84696560

1 20. The system as recited in claim 15, wherein the command for operation of the  
2 network device is encrypted, and wherein the cryptographic key is utilized to  
3 decrypt the command for operation.

1 21. The system as recited in claim 15, further comprising logic that receives  
2 electronic payment for paying for operation of the network device.

1 22. A method for secure identification of a network device, comprising:

2 (a) assigning a digital certificate to a network device;

3 (b) receiving a command for operation of the network device from a network  
4 user;

5 (c) sending the digital certificate to the network user, wherein the network user  
6 utilizes a cryptographic key to authenticate the digital certificate of the  
7 network device; and

8 (d) enabling operation of the network device if the digital certificate of the  
9 network device is authenticated.

1 23. The method as recited in claim 22, and further comprising establishing  
2 secure communication between the network device and an administrator of  
3 the device for at least one of a maintenance function and a billing function.

1 24. The method as recited in claim 23, and further comprising receiving a  
2 software update for the network device from the administrator.

1 25. The method as recited in claim 22, wherein the network user is another  
2 network device.

006T90" 84696560

1 26. The method as recited in claim 22, and further comprising assigning a unique  
2 digital certificate to a second network device, wherein the command for  
3 operation of the network device is re-routed to the second network device  
4 based on at least one of attributes of the network devices and a policy.

1 ~~27.~~ A method for secure management of a network device, comprising:

2 (a) associating at least one of policy information and a computational protocol  
3 with a command for the network device;

4 (b) encrypting the at least one of policy information and computational  
5 protocols;

6 (c) sending the at least one of policy information and computational protocols to  
7 the network device;

8 (d) decrypting the at least one of policy information and computational  
9 protocols; and

10 (e) processing the command with the network device utilizing the at least one of  
11 policy information and computational protocols.

0065948-161900